

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400



PATENT APPLICATION *AF Ifw*

ATTORNEY DOCKET NO. 10014006-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard Paul TARQUINI

Confirmation No.: 4897

Application No.: 10/003,747

Examiner: Perungavoor, Venkatanaray

Filing Date: October 31, 2001

Group Art Unit: 2132

Title: METHOD, COMPUTER READABLE MEDIUM, AND NODE FOR A THREE-LAYERED INTRUSION
PREVENTION SYSTEM FOR DETECTING NETWORK EXPLOITS

Mail Stop Appeal Brief - Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF REPLY BRIEF

Transmitted herewith is the Reply Brief with respect to the Examiner's Answer mailed on January 26, 2006.

This Reply Brief is being filed pursuant to 37 CFR 1.193(b) within two months of the date of the Examiner's Answer.

(Note: Extensions of time are not allowed under 37 CFR 1.136(a))

(Note: Failure to file a Reply Brief will result in dismissal of the Appeal as to the claims made subject to an expressly stated new ground rejection.)

No fee is required for filing of this Reply Brief.

If any fees are required please charge Deposit Account 08-2025.

☒ I hereby certify that this correspondence is being
deposited with the United States Postal Service
as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit: March 13, 2006

OR

☐ I hereby certify that this paper is being
transmitted to the Patent and Trademark Office
facsimile number (571) 273-8300.
Date of facsimile:

Typed Name: Cindy C. Dioso

Signature: Cindy C. Dioso

Respectfully submitted,

Richard Paul TARQUINI

By James L. Baudino

James L. Baudino

Attorney/Agent for Applicant(s)

Reg No. : 43,486

Date : March 13, 2006

Telephone : (214) 855-7544



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**APPEAL FROM THE EXAMINER TO THE BOARD
OF PATENT APPEALS AND INTERFERENCES**

In re Application of: Richard Paul TARQUINI Confirmation No: 4897

Serial No.: 10/003,747

Filing Date: October 31, 2001

Group Art Unit: 2132

Examiner: Perungavoor, Venkatanaray

Title: METHOD, COMPUTER READABLE MEDIUM, AND NODE
FOR A THREE-LAYERED INTRUSION PREVENTION
SYSTEM FOR DETECTING NETWORK EXPLOITS

Docket No.: 10014006-1

MAIL STOP: APPEAL BRIEF-PATENTS

Commissioner for Patents

P.O. Box 1450

Alexandria, Virginia 22313-1450

Dear Sir:

REPLY BRIEF

Applicant respectfully submits this Reply Brief in response to the Examiner's Answer mailed January 26, 2006, pursuant to 37 C.F.R. § 1.193(b).

As an initial matter, it has recently come to Applicant's attention that an appeal brief may be considered to be noncompliant with 37 C.F.R. § 41.37 if headings are not provided for each ground of rejection. While this has not happened in the present case, out of an abundance of caution, Applicant has provided herewith an Amended Appeal Brief containing such headings. No changes to the arguments have been made in the Appeal Brief from those presented in Applicant's Appeal Brief filed December 5, 2005.

STATUS OF CLAIMS

Claims 1-19 stand rejected pursuant to a Final Office Action mailed August 3, 2005. Claims 1-19 are presented for appeal.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 5-9 and 14-16 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter “*Vaidya*”).

2. Claims 2-4, 10-13 and 17-19 are rejected under 35 U.S.C. §103(a) as being unpatentable in view of U.S. Patent No. 6,279,113 to “*Vaidya*” in view of U.S. Patent No. 6,851,061 issued to Holland, III et al. (hereinafter “*Holland*”).

ARGUMENT

1. First Ground of Rejection (Claims 1, 5-9 and 14-16)

In the Examiner's Answer, the Examiner seems to assert that because it is purportedly known that an OSI model has seven layers, Applicant's claimed invention is thereby anticipated by any system that evaluates data corresponding to any one of the seven layers (Examiner's Answer, page 3). Applicant respectfully disagrees. As discussed in Applicant's Appeal Brief (and Amended Appeal Brief), *Vaidya* appears to disclose a virtual processor 36 that obtains a data packet from a queue and extracts MAC header information, IP header information, transport header information, and application information from the data packet (*Vaidya*, column 7, lines 18-24). The data extracted from the packet is then entered into a register cache 40 of *Vaidya* where the extracted data is used to create a session cache entry (*Vaidya*, column 8, lines 48-51). Applicants respectfully submit that extracting header information from a data packet retrieved from a queue is not the same as monitoring layer data by different layers of an intrusion prevention system as generally recited by Claims 1 and 9. To the contrary, the Examiner does not explicitly identify any disclosure in the *Vaidya* reference identifying any intrusion prevention mechanism in *Vaidya* having different layers.

Additionally, in the Examiner's Answer, the Examiner refers to a timer/counter of *Vaidya* being used for application monitoring (Examiner's Answer, page 4). Applicant respectfully submits that the portion of *Vaidya* referred to by the Examiner appears to relate to searching data in a state cache 44 for a matching entry, and that the session entry may contain a record of timer/counter expressions (used to determine whether a network intrusion is associated with a particular network packet) (*Vaidya*, column 9, lines 3-20). Thus, the portion of *Vaidya* referred to by the Examiner clearly does not disclose or even suggest any intrusion mechanism having different layers as generally recited by Claims 1 and 9.

The Examiner further refers to column 3, line 66 to column 4, line 26 of *Vaidya* which appears to disclose that three different types of attack signature profiles are used to detect a network intrusion. Again, Applicant respectfully submits that the portion of

Vaidya relied on by the Examiner fails to disclose or even suggest any intrusion mechanism having different layers as generally recited by Claims 1 and 9.

Specifically, the Examiner recites “*Vaidya* effectively discloses the monitoring of three layers” (Examiner’s Answer, page 4). Even if *Vaidya* is considered to disclose what the Examiner asserts, of which Applicant respectfully does not concur, Applicant respectfully submits that monitoring three layers does not automatically equate to an intrusion detection system having three layers as generally recited by Claims 1 and 9. Accordingly, Applicant respectfully submits that Claims 1 and 9, and Claims 5-8 and 14-16 that depend respectively therefrom, are allowable.

2. Second Ground of Rejection (Claims 2-4, 10-13 and 17-19)

Claims 2-4 and 10-13 depend respectively from independent Claims 1 and 9. At least for the reasons discussed above, independent Claims 1 and 9 are allowable. Moreover, *Holland* does not appear to remedy at least the deficiencies of *Vaidya* indicated above, nor did the Examiner rely on *Holland* to reject independent Claims 1 and 9. Therefore, Applicant respectfully submits that Claims 2-4 and 10-13 are patentable over the cited references.

In the Examiner’s Answer, the Examiner refers to various portions of *Holland* and states:

Holland discloses the layers having drivers . . . and further the drivers being in kernel space And further *Holland* discloses the media access control driver and intrusion prevention system transport service provider layer . . . where *Holland* mentions TCP/UDP data being shimmed. And *Holland* also discloses the media access control driver And the drivers and intrusion prevention system transport service provider layer being part of IP stack (network stack) of operating system

(Examiner’s Answer, page 5). Applicant respectfully submits that the Examiner’s statements appear to be nothing more than a random recitation of different portions of *Holland*, none of which disclose or even suggest “an operating system comprising a

network stack comprising a protocol driver, a media access control driver . . . and an intrusion prevention system transport service provider layer” as recited by Claim 17 (emphasis added). In fact, the Examiner appears to rely primarily on two different figures of *Holland*, namely, figures 2 and 3 (see the Examiner’s Answer’s recited portions of *Holland* and the Examiner’s Final Office Action). Specifically, figure 2 of *Holland*, which *Holland* identifies as “prior art,” appears to disclose a packet filter 37 which is relied on by the Examiner to reject independent Claim 17 (Final Office Action, page 6). However, such “packet filter 37” of *Holland* clearly does not form part of the IP stack 33 illustrated in figure 3 of *Holland*. Further, the Examiner’s reliance on column 5, lines 47–60, of *Holland* appears to relate to figure 3 of *Holland*. However, such portion of *Holland* referred to and relied on by the Examiner recites:

No packet filtering or other processing is performed. A network capture module 63 collects the message blocks for use by the analysis module 61.

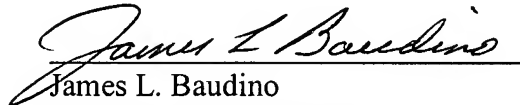
(*Holland*, column 5, lines 57-60). Referring to figure 3, the network capture module 63 and analysis module 61 clearly do not form part of the IP stack 53 illustrated in figure 3 of *Holland*. Nor does *Vaidya* remedy at least these deficiencies of *Holland*. Accordingly, for at least these reasons, Applicant respectfully submits that neither *Vaidya* nor *Holland*, alone or in combination, disclose, teach or suggest the limitations of independent Claim 17. Thus, Claim 17, and Claims 18 and 19 that depend therefrom, are allowable.

CONCLUSION

Applicant has demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicant respectfully requests the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

No fee is believed due with this Reply Brief. If, however, Applicant has overlooked the need for any fee, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,


James L. Baudino
Registration No. 43,486

Date: March 13, 2006

Correspondence To:

L. Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-3884